2017 Asia Pacific & Japan Cyber Risk Transfer Comparison Report

Sponsored by Aon Risk Solutions

Independently conducted by Ponemon Institute LLC

2017 Asia Pacific & Japan Cyber Risk Transfer Comparison Report

Sponsored by Aon Risk Solutions
Independently Conducted by Ponemon Institute LLC

Part 1. Introduction

The purpose of this research is to compare the relative insurance protection of certain tangible[1] versus intangible[2] assets. How do cyber asset values and potential losses compare to tangible asset values and potential losses from an organization's other perils, such as fires and weather?

The probability of any particular building burning down is significantly lower than one percent (1%). However, most organizations spend much more on fire-insurance premiums than on cyber insurance despite stating in their publicly disclosed documents that a majority of the organization's value is attributed to intangible assets.[3] One recent concrete example is the sale of Yahoo!: Verizon recently reduced the purchase price by $350 million because of the severity of cyber incidents in 2013 and 2014.

Acceleration in the scope, scale and economic impact of technology multiplied by the concomitant data revolution, which places unprecedented amounts of information in the hands of consumers and businesses alike, and the proliferation of technology-enabled business models,[4] force organizations to examine the benefits and consequences of emerging technologies.[5]

This financial-statement quantification study demonstrates that organizations recognize the growing value of technology and data assets relative to historical tangible assets, yet a disconnect remains regarding cost-benefit analysis resource allocation. Particularly, a disproportionate amount is spent on tangible asset insurance protection compared to cyber asset protection[6] based on the respective relative financial statement impact and potential expected losses.[7]

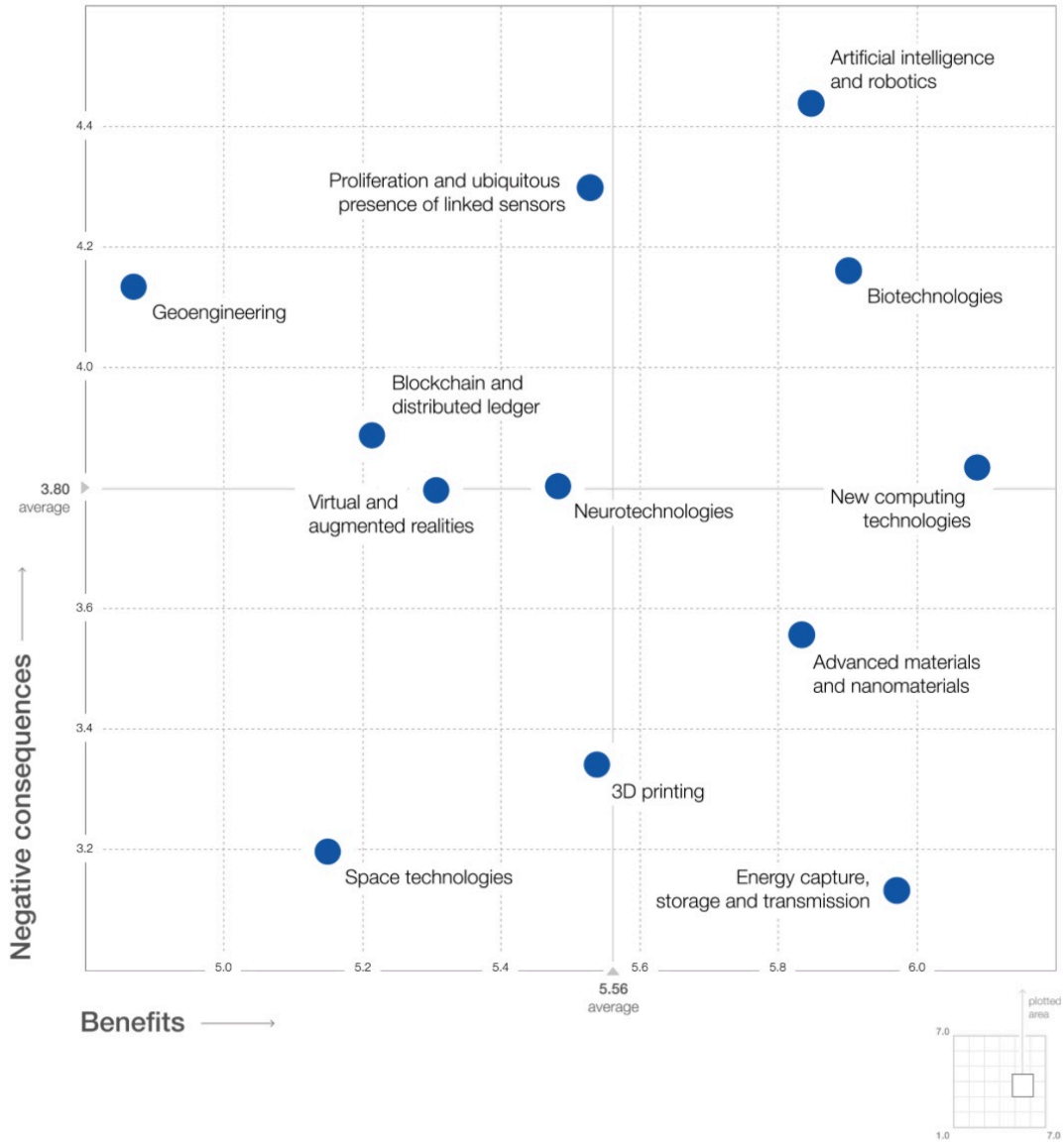
Quantitative models are being developed that evaluate the return on investment of various cyber risk management IT security and process solutions, which can incorporate cost-benefit analysis for different levels of insurance.[8] As such, organizations are driven toward a holistic capital expenditure discussion spanning functional teams rather than being segmented in traditional siloes. The goal of these models is to identify and protect critical assets by aligning macro-level risk tolerance more consistently.

---

[1] Property, Plant & Equipment (PP&E)
[2] Computer systems and related digital assets. Most other cyber-incident studies include damage estimates of subjective intangible assets that are difficult to quantify and almost impossible to insure, such as brand and reputation. Furthermore, the value of trade secrets and patent infringement are typically excluded from cyber insurance, although there are new models being developed to quantify intangible intellectual property values, which could eventual lead to viable insurance in the near future.
[3] More than 80% of a company's value is derived from intangible assets according to some studies.
[4] No Ordinary Disruption: The Four Global Forces Breaking All the Trends. McKinsey Global Institute.
[5] Source: World Economic Forum Global Risks Perception Survey
[6] Aon has placed primary cyber insurance with 67 different insurance carriers, which entails 67 different insurance applications, underwriting processes, policy form wording, servicing capabilities and claims payment aptitude.
[7] Unfortunately, it is not a binary discussion because property, general liability, crime, kidnap & ransom and other lines of insurance may intentionally or unintentionally include elements of cyber coverage.
[8] A 2016 Rand Study found contrary results: "Cost of Cyber Incidents Not Large Compared with Other Business Losses; May Influence Responses by Businesses"

An interesting perspective on the perceived benefits and negative consequences of 12 emerging technologies is the *Global Risks Report* published by the World Economic Forum (WEF), as shown in Figure 1. This year, the WEF's Global Risks Perception Survey considered the impact of 12 emerging technologies.[9] While the results suggest that the benefits of these technologies outweigh the negative consequences, there is a need for better governance of emerging technologies.

Figure 1. Examining the risk: Benefit analysis of intangible & intangible assets



Source: World Economic Forum Global Risks Perception Survey 2016.

[9] World Economic Forum Global Risks Perception Survey
http://reports.weforum.org/global-risks-2017/part-3-emerging-technologies/3-1-understanding-the-risk-landscape/

How do organizations qualify and quantify the corresponding impact of financial statement exposure? Our goal is to compare the financial statement impact of tangible property and network risk exposures. A better understanding of the relative financial statement impact will assist organizations in allocating resources and determining the appropriate amount of risk transfer (insurance) resources to allocate to the mitigation of the financial statement impact of network risk exposures.

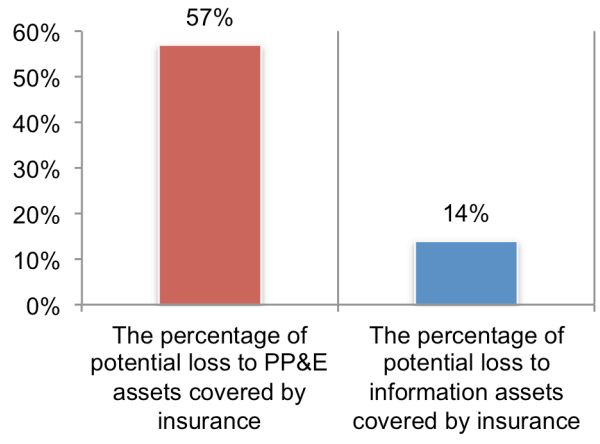
Network risk exposures can broadly include breach of privacy and security of personally identifiable information, stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on computers, posting confidential business information on the Internet, robotic malfunctions and disrupting a country's critical national infrastructure.[10]

We surveyed 520 individuals in Asia Pacific and Japan[11] involved in their company's cyber risk management as well as enterprise risk management activities. Most respondents are either in finance, treasury and accounting (29 percent of respondents) or risk management (26 percent of respondents). Other respondents are in corporate compliance/audit (13 percent of respondents) and general management (13 percent of respondents).

All respondents are familiar with the cyber risks facing their company. In the context of this research, cyber risk means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.[12]

As shown in Figure 2, despite the greater average potential loss to information assets ($939 million) compared to Property, Plant & Equipment (PP&E) ($739 million), the latter has much higher insurance coverage (57 percent vs. 14 percent).

Figure 2. The percentage of PP&E and information assets covered by insurance



Following are some of the key takeaways from this research:

- Information assets are underinsured against theft or destruction based on the value, probable maximum loss (PML) and likelihood of an incident.
- Disclosure of a material loss of PP&E and disclosure of information assets differ. Forty percent of respondents say their company would disclose the loss of PP&E in its financial statements as a footnote disclosure. However, 35 percent of respondents say a material loss to information assets does not require disclosure.
- Despite the risk, companies are reluctant to purchase cyber insurance coverage. Sixty-two percent of respondents believe their company's exposure to cyber risk will increase over the

[10] Even though some network risks, also known as cyber risks, are not yet fully insurable via traditional insurance markets (e.g. the ***value*** of trade secrets) and other cyber risks may be insurable under legacy policies (e.g. property, general liability, crime, etc.), it is useful to understand the relative risks in in terms of enterprise management of financial statement impact.
[11] Countries included in this report are ANZ,ASEAN (cluster), Hong Kong, India, Japan, Korea and Taiwan
[12] Source: Institute of Risk Management

next 24 months. However, only 18 percent of respondents say their company has cyber insurance coverage.

- Forty-one percent of companies represented in this study experienced a material or significantly disruptive security exploit or data breach one or more times during the past two years, with an average economic impact of $3.3 million.

- Eighty-six percent of respondents believe cyber liability is one of the top 10 business risks for their company.

Part 2. Key findings

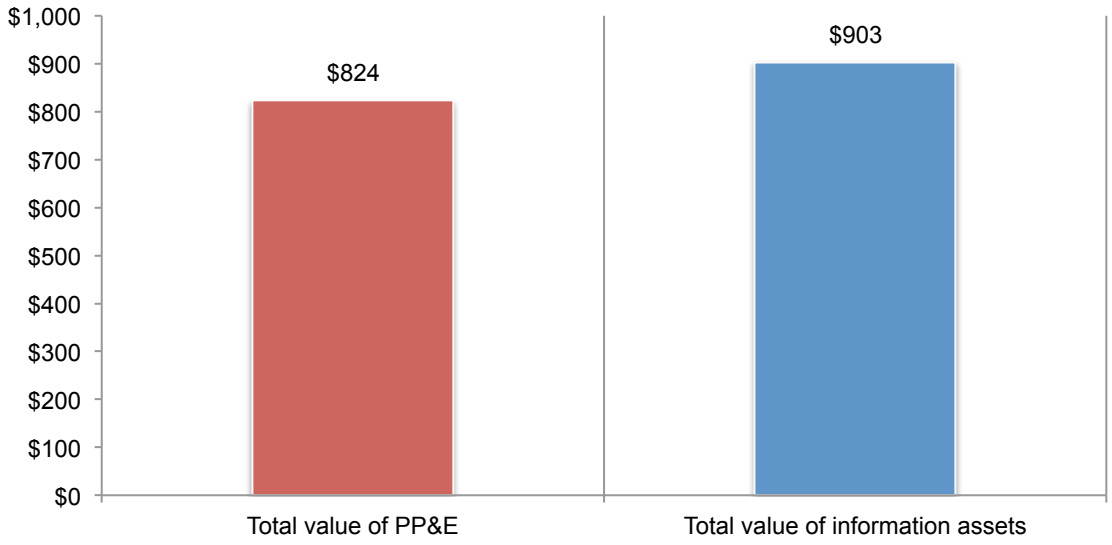
The complete audited findings are presented in the appendix of this report. We have organized the report according to the following topics:

- Differences between the valuation and PML of PP&E and information assets
- The cyber risk experience of companies
- Perceptions about the financial impact of cyber exposures

Differences between the valuation and PML of PP&E and information assets

Companies value information assets slightly higher than they do PP&E[13]. According to Figure 3, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems is approximately $824 million for the companies represented in this research. The average total value of information assets, which includes customer records, employee records, financial reports, analytical data, source code, models methods and other intellectual property, is slightly more than PP&E ($903 million).

Figure 3. The total value of PP&E and information assets
Extrapolated value ($ millions)

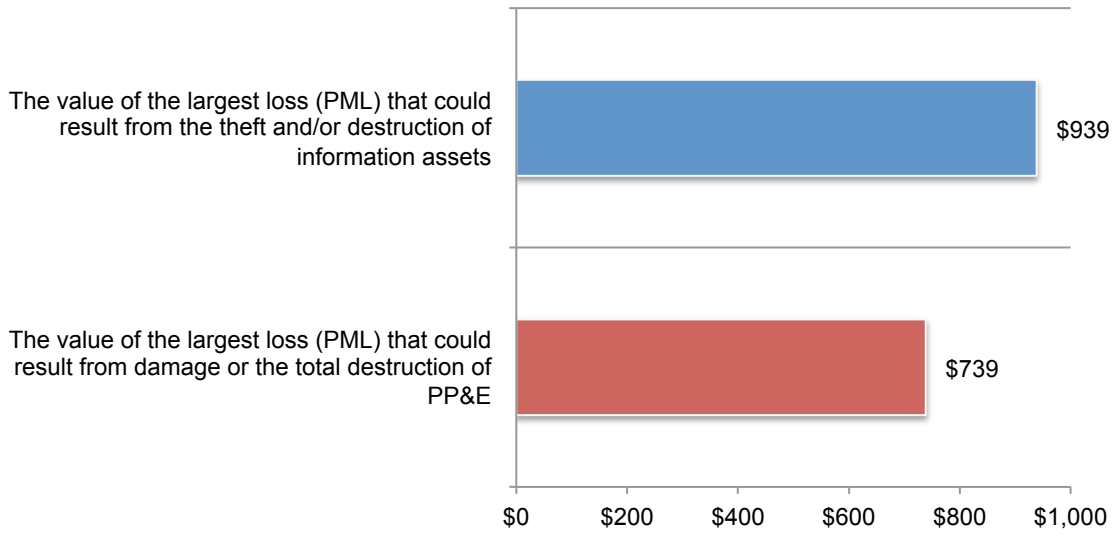


[13] Respondents were asked to assume, with respect to PP&E assets, the root causes of loss (a.k.a. perils) include fire, flooding, weather events, earthquakes and other natural or man-made disasters.

The value of probable maximum loss (PML)[14] is higher for information assets than PP&E. Companies estimate the PML if information assets are stolen or destroyed at an average of approximately $939 million, according to Figure 4. This assumes the normal functioning of passive protective cybersecurity solutions such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.

In contrast, the value of the largest loss that could result from damage or total destruction of PP&E is approximately $739 million on average. This also assumes the normal functioning of passive protective features such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.

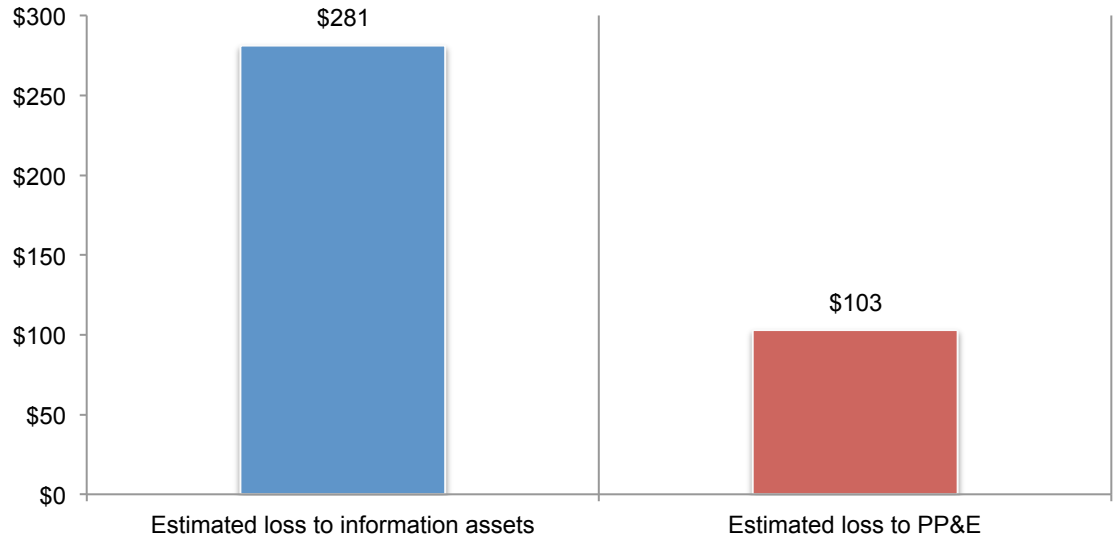
Figure 4. The PML value for PP&E and information assets
Extrapolated value ($ millions)



[14] Probable Maximum Loss (PML) is defined as the value of the largest loss that could result from a disaster, assuming the normal functioning of passive protective features (i.e. firewalls, nonflammable materials, etc.) and proper functioning of most (perhaps not all) active suppression systems (i.e. sprinklers).

What is the impact of business disruption to PP&E and information asset losses?
According to Figure 5, business disruption has a greater impact on information assets ($281 million)[15] than on PP&E ($103 million).

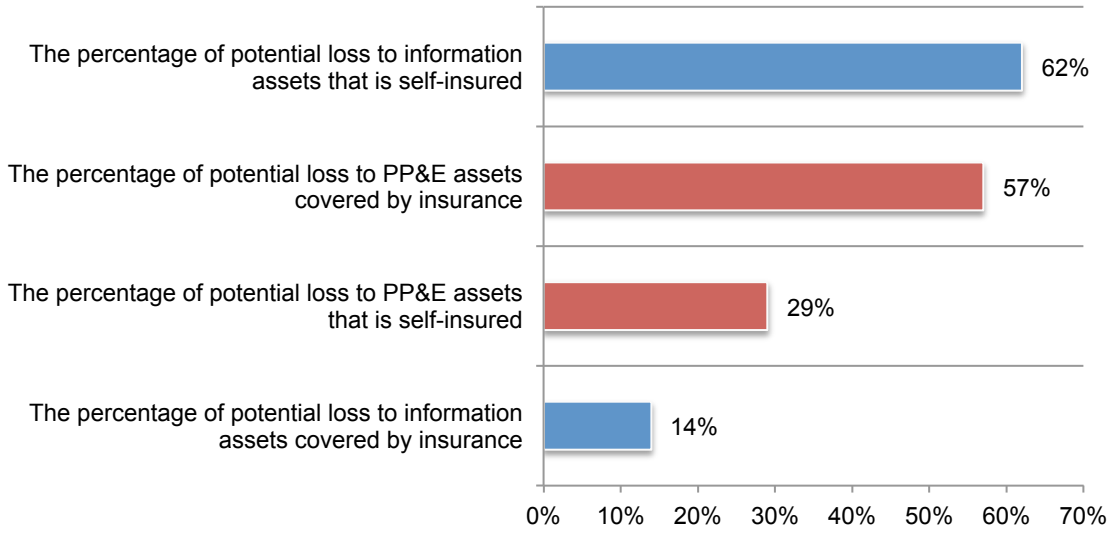
Figure 5. The impact of business disruption to information assets and PP&E
Extrapolated value ($ millions)



[15] While the survey results suggest Probable Maximum Loss in the neighborhood of $281 million, a growing number of companies are using Risk Decision Platform Analysis and Cyber Modeling to suggest potential losses in excess of $500 million to over $1 billion and seek cyber insurance limit premium quotes and policy terms for such amounts.

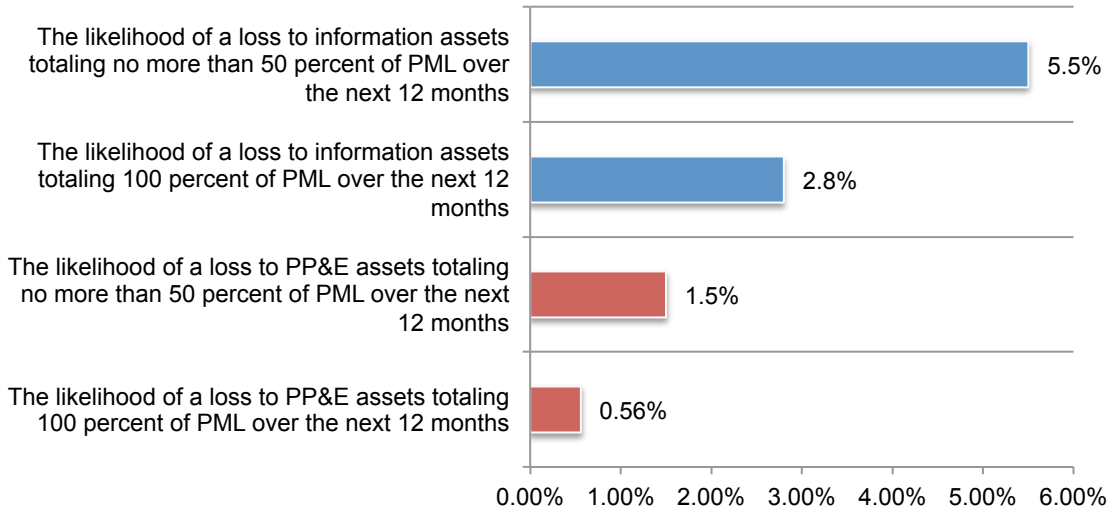
There is a significant difference between the insurance coverage of PP&E and information assets. On average, approximately 57 percent of PP&E assets are covered by insurance and approximately 29 percent of PP&E assets are self-insured (Figure 6)[16]. In contrast, an average of 14 percent of information assets are covered by insurance. Self-insurance is higher for information assets at 62 percent.

Figure 6. Percentage of PP&E and information assets covered by insurance
Extrapolated percentage



The likelihood of a loss is higher for information assets than for PP&E. Companies estimate the likelihood that they will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months at 5.5 percent and 100 percent of PML at 2.8 percent, as shown in Figure 7. The likelihood of a loss to PP&E totaling no more than 50 percent of PML over the next 12 months is an average of 1.5 percent and at 100 percent of PML it is 0.56 percent.

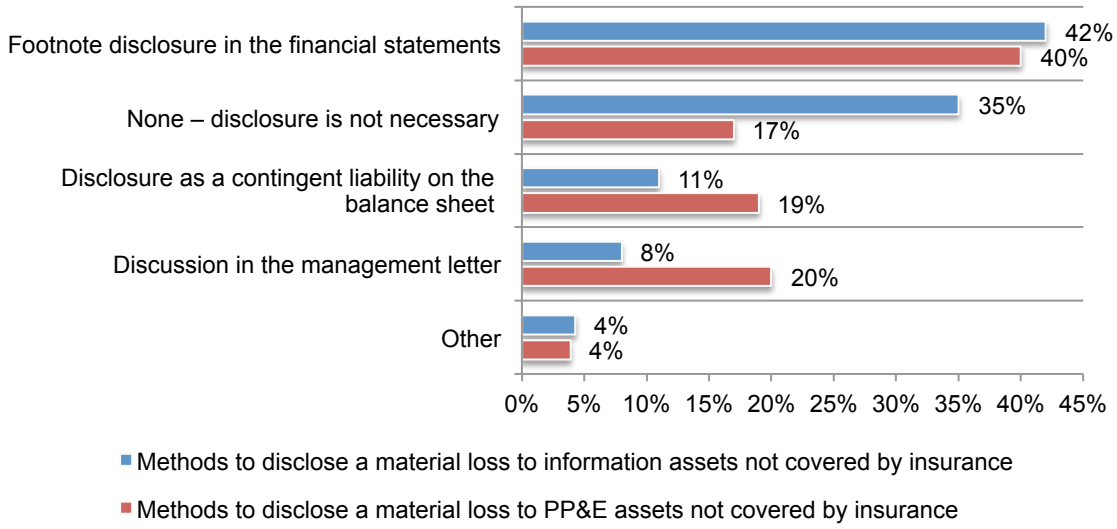
Figure 7. Likelihood of loss to PP&E and information assets totaling more than 50 percent and 100 percent of PML over the next 12 months
Extrapolated percentage



[16] The percentages do not add up to 100 percent because they are extrapolated values from questions 3,4,10 and 11. These results are shown in the complete audited findings in the appendix of the report.

Disclosure of material loss to PP&E and disclosure of material loss to information assets also differs. Figure 8 focuses on how companies would disclose a material loss. Forty percent of respondents say their company would disclose a material loss to PP&E assets that is not covered by insurance in its financial statements as a footnote disclosure in the financial statement, followed by a disclosure as a contingent liability on the balance sheet, such as FASB 5, (19 percent of respondents). Forty-two percent say they would disclose a material loss to information assets as a footnote disclosure in the financial statements, but 35 percent of respondents do not believe disclosure would be necessary.

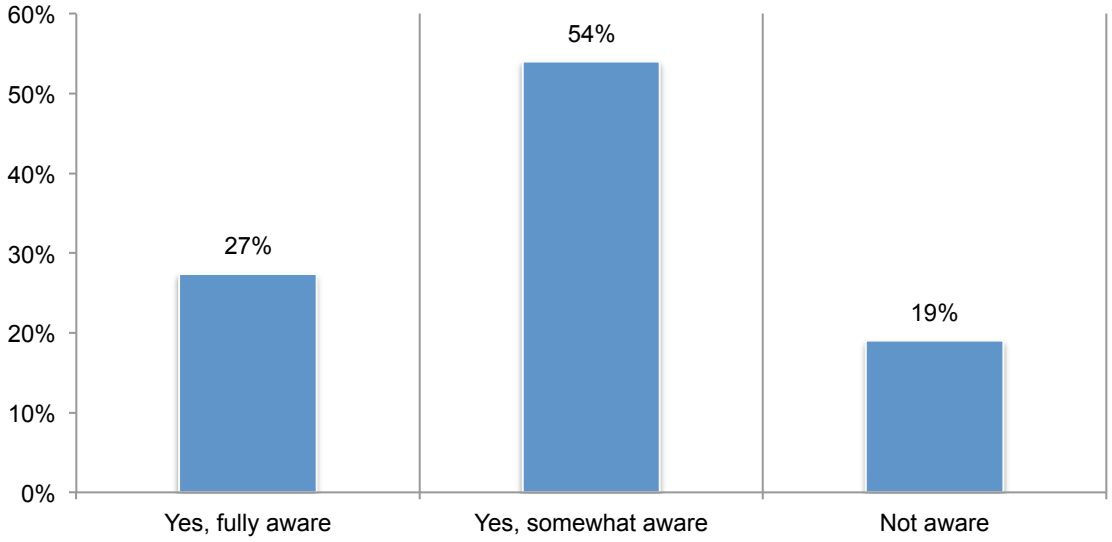
Figure 8. How would your company disclose a material loss to PP&E and information assets?



The cyber risk experience of companies

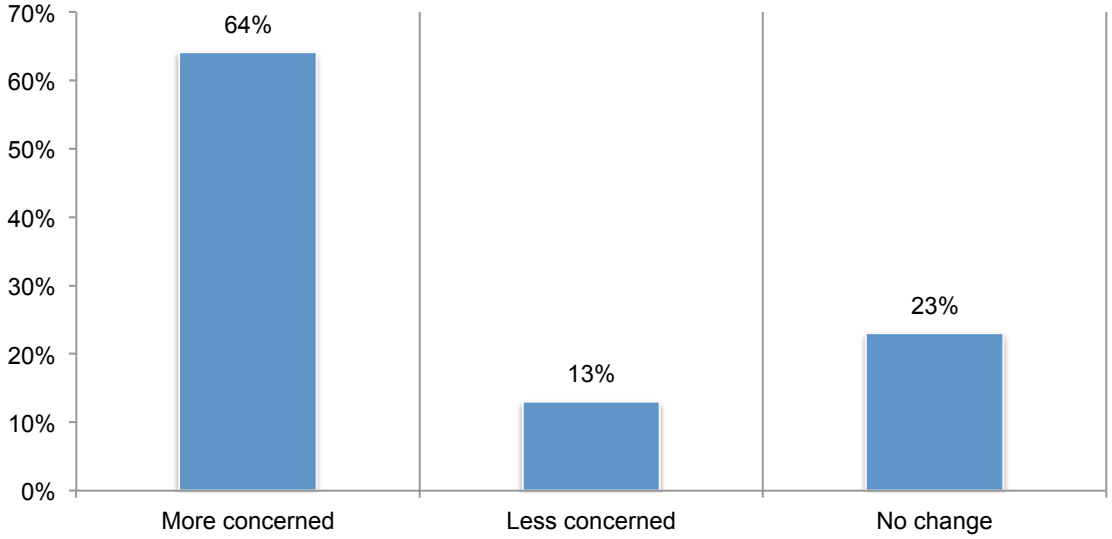
Awareness of the economic and legal consequences of an international data breach or security exploit is low. As revealed in Figure 9, only 27 percent of respondents are fully aware of the potential consequences of a data breach or security exploit in other countries in which their company operates, with 19 percent responding that they are not aware of the consequences.

Figure 9. Awareness of the economic and legal consequences of an international data breach or security exploit



Many companies had a material[17] or significantly disruptive security exploit or data breach one or more times in the past 24 months. Forty-one percent of respondents report their company had such a security incident. The average total financial impact of these incidents was $3.3 million.[18] As Figure 10 indicates, 64 percent of these respondents say the incident increased their company's concerns over cyber liability.

Figure 10. How did the security exploit or data breach affect your company's concerns over cyber liability?

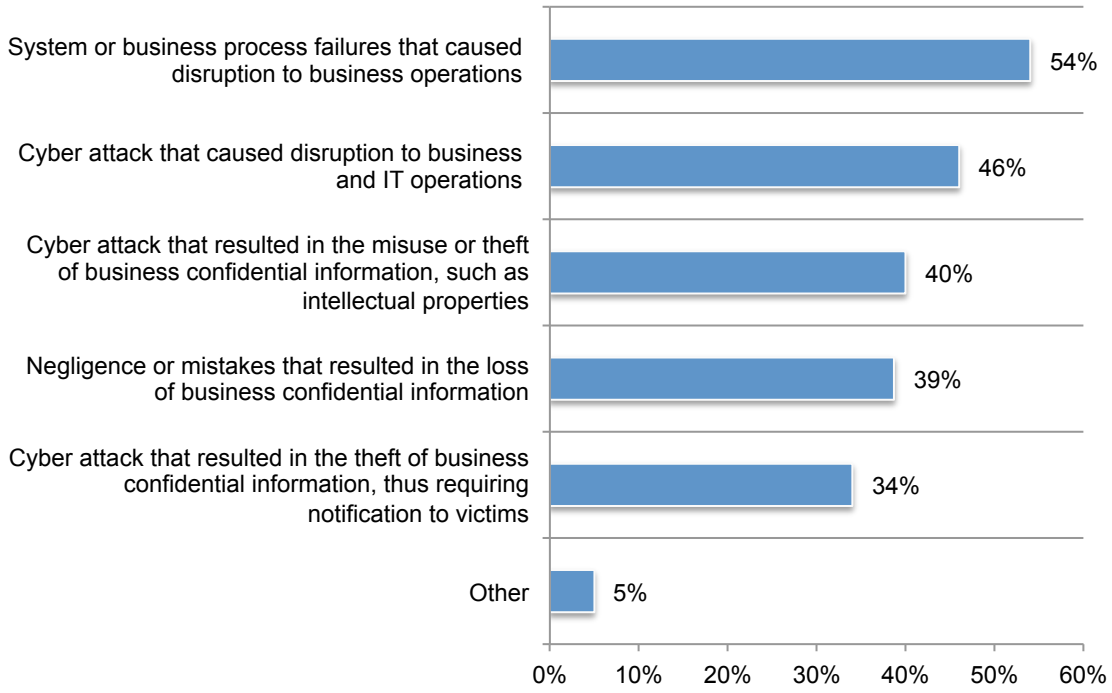


[17] In the context of this study, the term materiality takes into consideration monies expended for first-party losses, potential third-party liabilities, value of lost time, litigation costs, reputation damages and revenue losses. This term is broader than materiality as defined by GAAP and SEC requirements.
[18] This included all costs, including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.

The types of security incidents that 41 percent of the companies in this research faced are displayed in Figure 11. The most frequent type of incident was a system or business process failures that caused disruption to business operations (54 percent of respondents); this is followed by 46 percent of respondents who say the most frequent type of incident is a cyber attack that caused disrupt to business and IT operations.

Incidents involving the loss or theft of information assets were not as prevalent as those causing business disruptions. Forty percent say the cyber attack resulted in the misuse or theft of business confidential information, such as intellectual properties, and 39 percent of respondents say the incident involved negligence or mistakes that resulted in the loss of business confidential information.

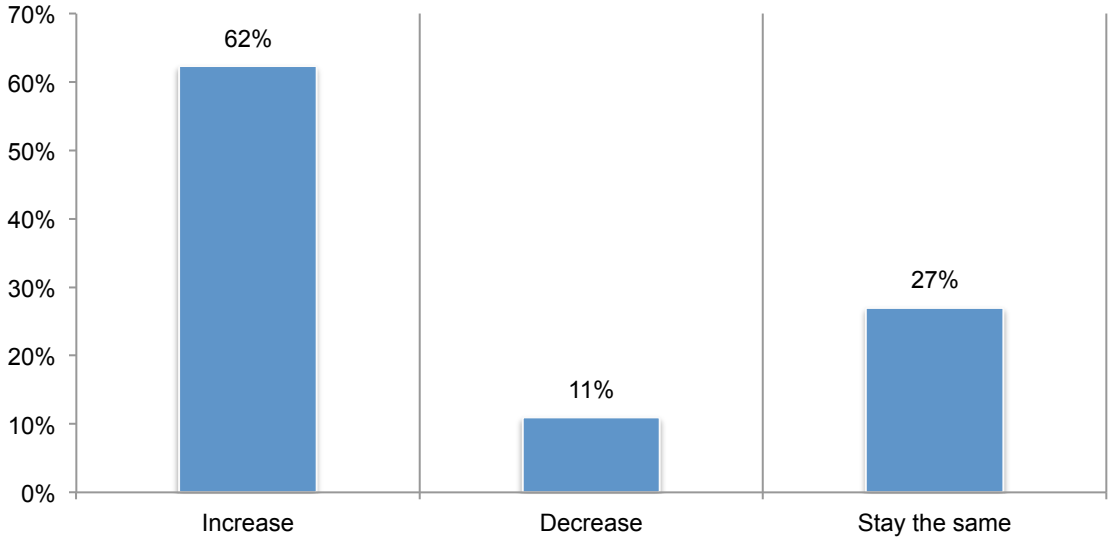
Figure 11. What type of data breach or security exploit did your company experience?
More than one response allowed



Perceptions about the financial impact of cyber exposures

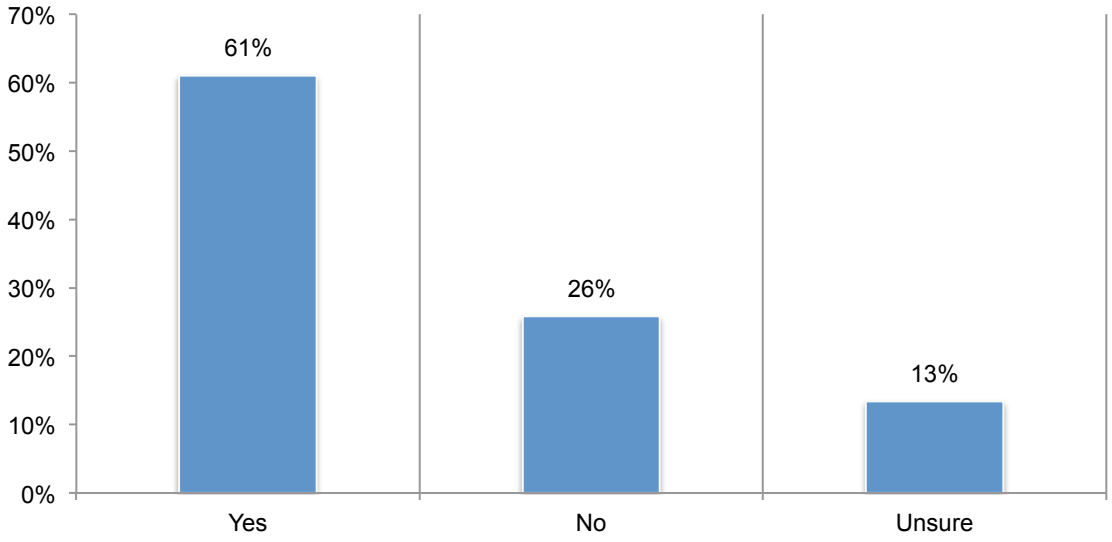
Companies' exposure to cyber risk is expected to increase; yet 41 percent of respondents say there is no plan to purchase cyber insurance. As the data in Figure 12 show, 62 percent of respondents believe their companies' exposure to cyber risk will increase and 27 percent of respondents say it will stay the same. Only 11 percent of respondents expect it to decrease.

Figure 12. Will your company's cyber risk exposure increase, decrease or stay the same over the next 24 months?



Despite the extent of cyber risk, which exceeds that of PP&E risk, only 18 percent of respondents say their companies currently have cyber insurance coverage with an average limit of approximately $13 million. As Figure 13 reveals, 61 percent of respondents believe this insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security.

Figure 13. Is your company's cyber insurance coverage sufficient?



According to Figure 14, the adequacy of coverage is determined mainly by a formal risk assessment conducted by a third party (26 percent of respondents) followed by the maximum available from the insurance market (21 percent of respondents). Only 11 percent say it was determined by a formal risk assessment conducted by the insurer, and 13 percent say it was a formal risk assessment by in-house staff.

Figure 14. How companies determine the adequacy of coverage

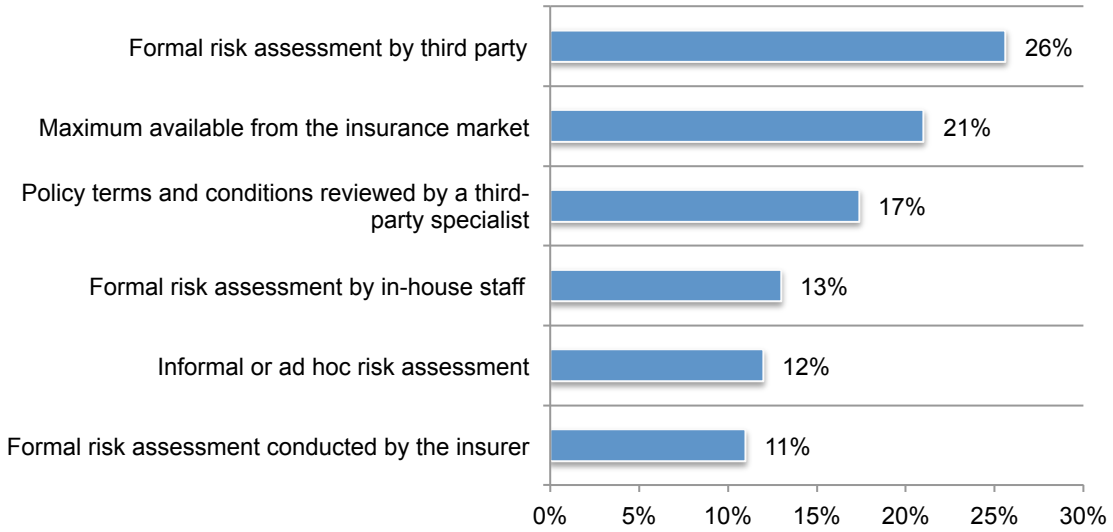
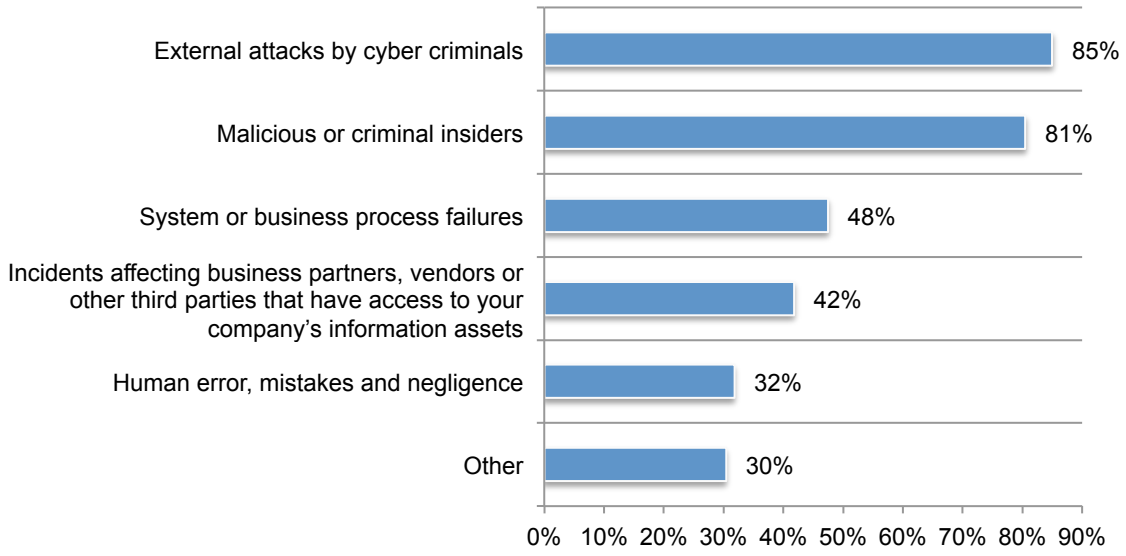


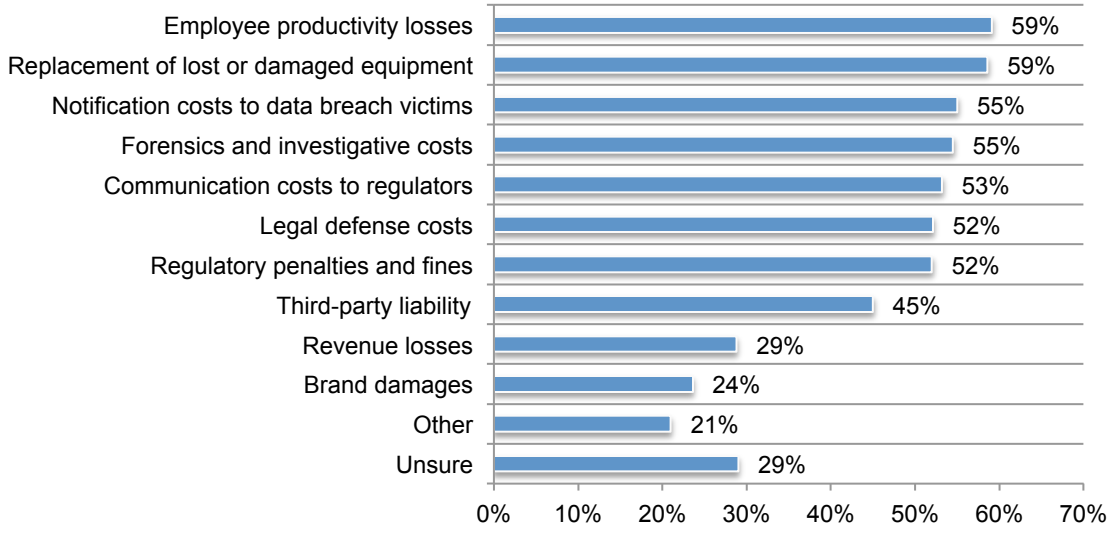
Figure 15 displays the incidents typically covered by cyber insurance. Most incidents covered are external attacks by cyber criminals (85 percent of respondents) and attacks by malicious or criminal insiders (85 percent of respondents) and incidents causing system or business process failures (48 percent of respondents). Only 32 percent of respondents say the insurance covers incidents involving human error, mistakes and negligence.

Figure 15. Types of incidents covered by cyber insurance
More than one response allowed



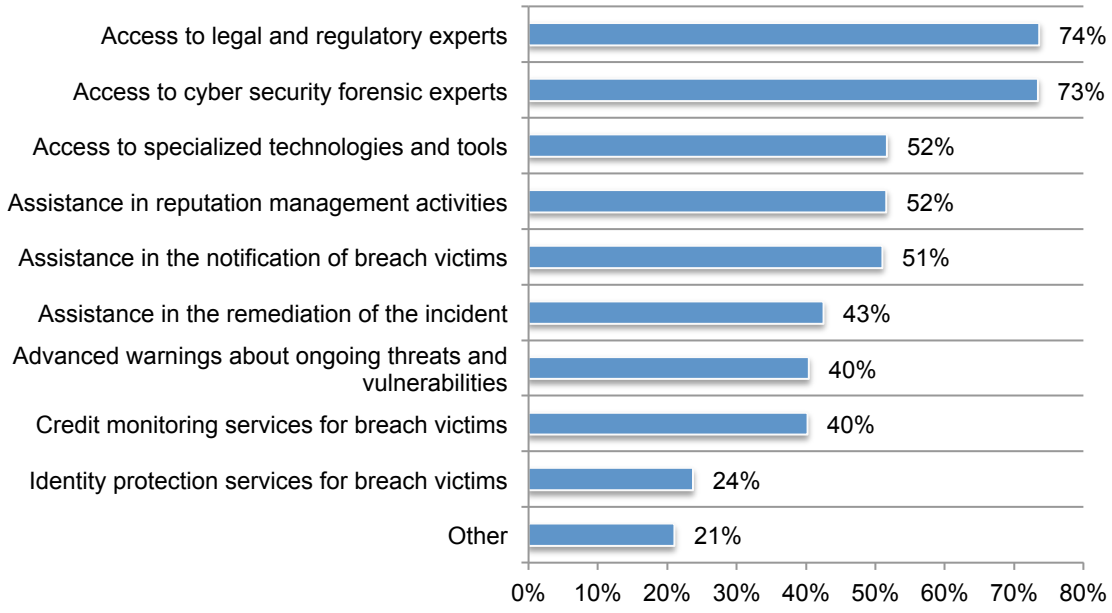
Figures 16 and 17 present the coverage and services provided by insurance companies. The top five costs covered are: employee productivity losses (59 percent of respondents), replacement of lost or damaged equipment (59 percent of respondents), notification costs to data breach victims (55 percent of respondents), forensics and investigative costs (55 percent of respondents and communication costs to regulators (53 percent of respondents).

Figure 16. Coverage provided by the insurance company
More than one response allowed



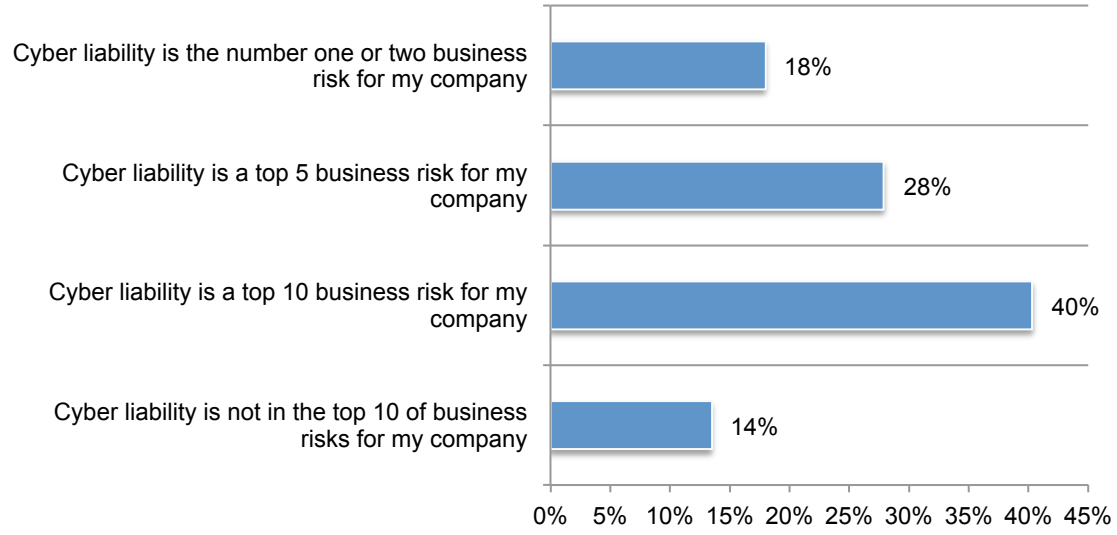
In addition to this coverage, other services provided are: access to legal and regulatory experts (74 percent of respondents), access to cyber security forensic experts assistance (73 percent of respondents), access to specialized technologies and tools and assistance in reputation management activities (both 52 percent of respondents), as shown in Figure 17.

Figure 17. Other services provided by the cyber insurer
More than one response allowed



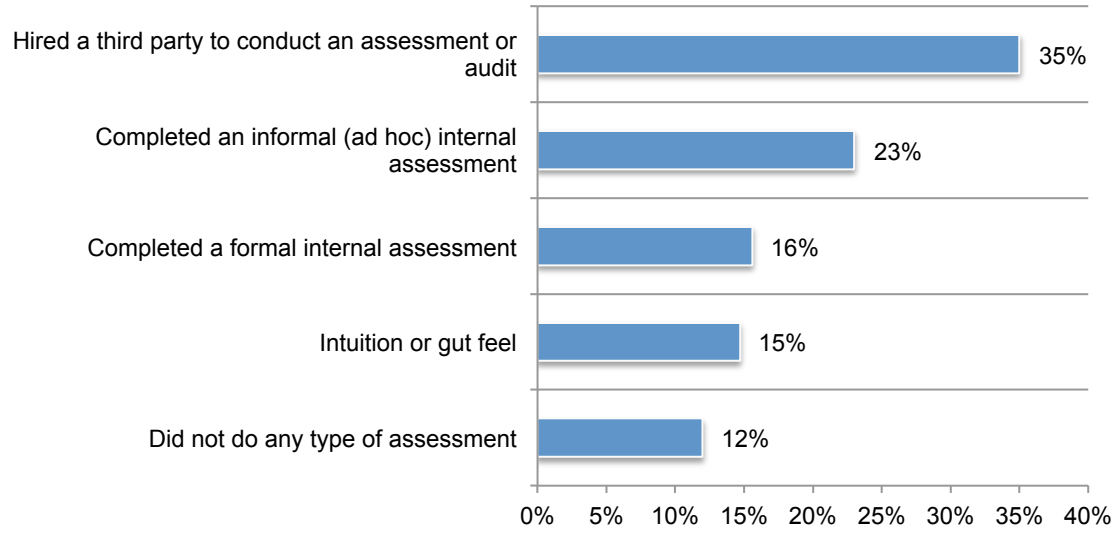
Cyber liability ranks in the top 10 of all business risks facing companies. Figure 18 demonstrates that only 14 percent of respondents do not consider cyber risk as a top 10 risk for their companies. Twenty-eight percent of respondents place this risk in the top five, and 40 percent of respondents place it in the top 10.

Figure 18. How do cyber risks compare to other business risks?



To determine the cyber risk to their company, 35 percent of respondents say the company hired a third-party to conduct an assessment or audit and 23 percent of respondents say it was an informal (ad hoc) internal assessment (Figure 19). Only 16 percent of respondents say their company completed a formal internal assessment, and 15 percent of respondents say it was intuition or gut feel.

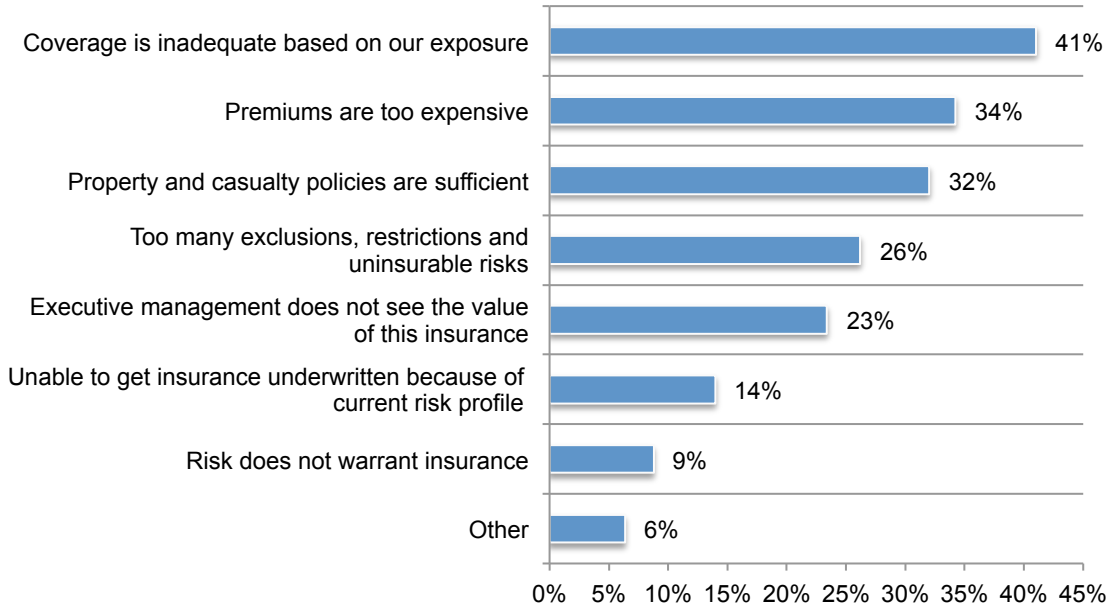
Figure 19. How did you determine the level of cyber risk to your company?



Will the purchase of stand alone cyber insurance increase because of concerns about security exploits and data breaches? Twelve percent of respondents say their company will purchase cyber insurance in the next 12 months, 27 percent of respondents say they will in the next two years and 20 percent of respondents say they will in more than two years.

According to Figure 20, the main reasons for not purchasing cyber security insurance are: coverage is inadequate based on exposure (41 percent of respondents), premiums are too expensive (34 percent of respondents) and property and casualty policies are sufficient (32 percent of respondents).

Figure 20. What are the main reasons why your company will not purchase stand alone cyber security insurance?
More than one response allowed



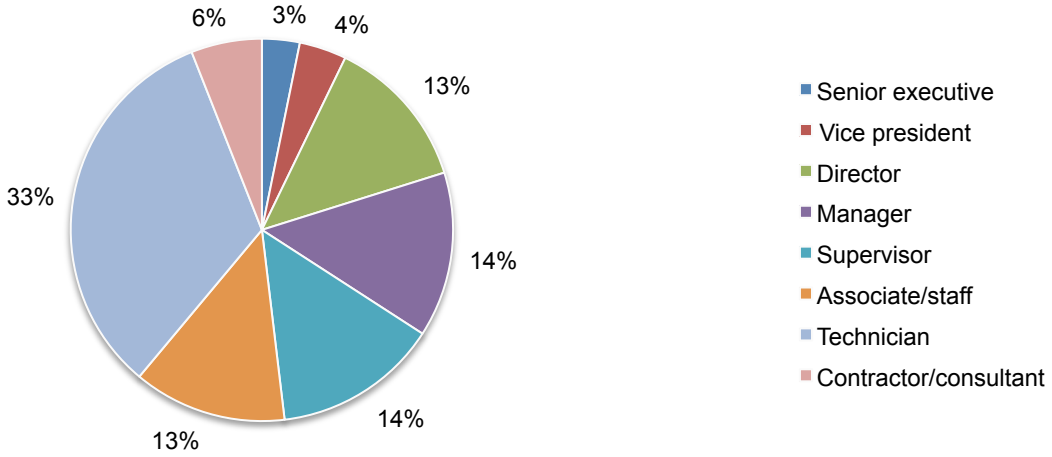
Part 3. Methods

The sampling frame is composed of 13,202 individuals who are involved in their company's cyber risk and enterprise risk management activities. As Table 1 shows, 568 respondents completed the survey. Screening removed 48 surveys. The final sample consisted of 520 surveys (a 3.9 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	13,202	100.0%
Total returns	568	4.3%
Rejected or screened surveys	48	0.4%
Final sample	520	3.9%

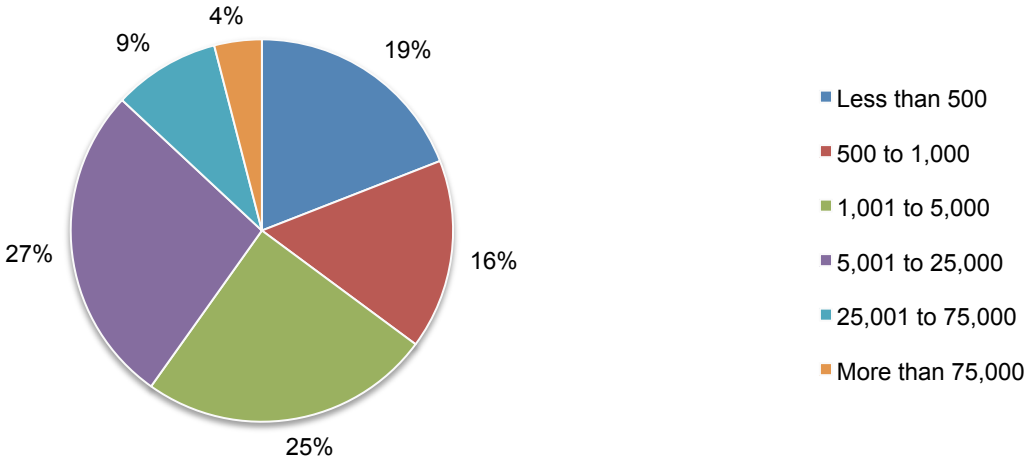
Pie Chart 1 reports the current position or organizational level of the respondents. Almos half of respondents (48 percent) reported their current position as supervisory level or above.

Pie Chart 1. Current position or organizational level



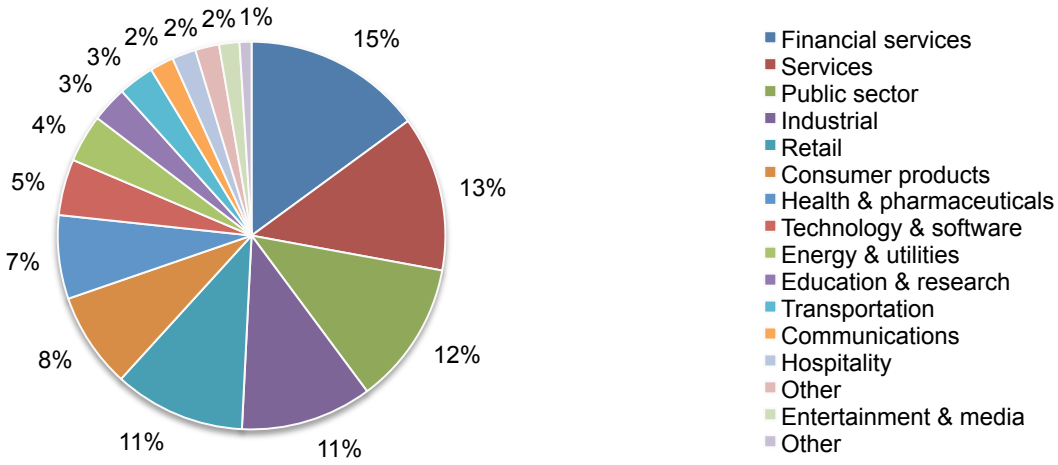
As Pie Chart 2 reveals, 65 percent of the respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (15 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (13 percent of respondents) and public sector (12 percent of respondents).

Pie Chart 3. Primary industry focus



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are involved in their company's cyber and enterprise risk management. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between December 2016 and February 2017.

Survey response	APJ 2017
Sampling frame	13,202
Total returns	568
Final sample	520
Response rate	3.9%
Sample weights	24.0%

Screening questions

S1. How familiar are you with cyber risks facing your company today?	APJ 2017
Very familiar	21%
Familiar	39%
Somewhat familiar	40%
Not familiar (stop)	0%
Total	100%

S2. Are you involved in your company's cyber risk management activities?	APJ 2017
Yes, significant involvement	23%
Yes, some involvement	77%
No involvement (stop)	0%
Total	100%

S3. Are you involved in your company's enterprise risk management activities?	APJ 2017
Yes, significant involvement	40%
Yes, some involvement	60%
No involvement (stop)	0%
Total	100%

S4. What best defines your role?	APJ 2017
Risk management	26%
Finance, treasury & accounting	29%
Corporate compliance/audit	13%
Security/information security	13%
General management	13%
Legal (OGC)	7%
None of the above (stop)	0%
Total	100%

The following questions pertain to your company's property, plant and equipment (PP&E)
Part 1. Sizing the economic impact

Q1. What is the total value of your company's PP&E, including all fixed assets plus SCADA and industrial control systems? Please exclude and assume a value based on full replacement cost (and not historic cost).	APJ 2017
Less than $1 million	4%
$1 to 10 million	14%
$11 to 50 million	15%
$51 to 100 million	24%
$101 to 500 million	24%
$501 to 1 billion	11%
$1 to 10 billion	4%
More than $10 billion	4%
Total	100%
Extrapolated value	823.83

Q2a. What is the value of the largest loss (PML) that could result from damage or the total destruction of PP&E. Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	APJ 2017
Less than $1 million	7%
$1 to 10 million	9%
$11 to 50 million	17%
$51 to 100 million	33%
$101 to 500 million	16%
$501 to 1 billion	10%
$1 to 10 billion	6%
More than $10 billion	3%
Total	100%
Extrapolated value	738.63

Q2b. What is the value of your largest loss (PML) due to business interruption? Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	APJ 2017
Less than $1 million	19%
$1 to 10 million	25%
$11 to 50 million	26%
$51 to 100 million	22%
$101 to 500 million	6%
$501 to 1 billion	2%
$1 to 10 billion	0%
More than $10 billion	0%
Total	100%
Extrapolated value	102.93

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	APJ 2017
Less than 5%	1%
5% to 10%	2%
11%to 20%	5%
21% to 30%	7%
31% to 40%	10%
41% to 50%	11%
51% to 60%	18%
61% to 70%	13%
71% to 80%	14%
81% to 90%	11%
91% to 100%	8%
Total	101%
Extrapolated value	57%

Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured?	APJ 2017
Less than 5%	10%
5% to 10%	14%
11% to 20%	15%
21% to 30%	16%
31% to 40%	15%
41% to 50%	12%
51% to 60%	6%
61% to 70%	7%
71% to 80%	3%
81% to 90%	1%
91% to 100%	0%
Total	99%
Extrapolated value	29%

Q5. What is the likelihood that your company will sustain a loss to PP&E assets totaling no more than 50 percent of PML over the next 12 months?	APJ 2017
Less than 0.1%	19%
0.1% to 0.5%	15%
0.6% to 1.0%	19%
1.1% to 2.0%	15%
2.1% to 3.0%	18%
3.1% to 4.0%	8%
4.1% to 5.0%	6%
5.1% to 10.0%	1%
More than 10.0%	0%
Total	100%
Extrapolated value	1.5%

Q6. What is the likelihood that your company will sustain a loss to PP&E assets totaling 100 percent of PML over the next 12 months?	APJ 2017
Less than 0.1%	66%
0.1% to 0.5%	12%
0.6% to 1.0%	9%
1.1% to 2.0%	6%
2.1% to 3.0%	2%
3.1% to 4.0%	1%
4.1% to 5.0%	1%
5.1% to 10.0%	2%
More than 10.0%	0%
Total	100%
Extrapolated value	0.56%

Q7. In your opinion, how would your company disclose a material loss to PP&E assets that is not covered by insurance in its financial statements?	APJ 2017
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	19%
Footnote disclosure in the financial statements	40%
Discussion in the management letter	20%
None – disclosure is not necessary	17%
Other	4%
Total	100%

The following questions pertain to your company's information assets.

Q8. What is the total value of your company's information assets, including customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties? Please assume a value based on full replacement cost (and not historic cost). Please note this value can be a precise quantification or estimate.	APJ 2017
Less than $1 million	7%
$1 to 10 million	12%
$11 to 50 million	17%
$51 to 100 million	25%
$101 to 500 million	19%
$501 to 1 billion	10%
$1 to 10 billion	7%
More than $10 billion	4%
Total	100%
Extrapolated value	903.40

Q9a. What is the value of the largest loss (PML) that could result from the theft and/or destruction of information assets. Please assume the normal functioning of passive protective cybersecurity features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.	APJ 2017
Less than $1 million	10%
$1 to 10 million	13%
$11 to 50 million	15%
$51 to 100 million	24%
$101 to 500 million	17%
$501 to 1 billion	10%
$1 to 10 billion	7%
More than $10 billion	4%
Total	100%
Extrapolated value	938.71

Q9b. What is the value of your largest loss (PML) due to cyber business interruption? Please assume the normal functioning of passive protective features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.	APJ 2017
Less than $1 million	19%
$1 to 10 million	25%
$11 to 50 million	21%
$51 to 100 million	17%
$101 to 500 million	9%
$501 to 1 billion	7%
$1 to 10 billion	4%
More than $10 billion	0%
Total	101%
Extrapolated value	281.22

Q10. What percentage of this potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured?	APJ 2017
Less than 5%	34%
5% to 10%	38%
11% to 20%	11%
21% to 30%	5%
31% to 40%	3%
41% to 50%	2%
51% to 60%	4%
61% to 70%	1%
71% to 80%	0%
81% to 90%	2%
91% to 100%	0%
Total	100%
Extrapolated value	0.14

Q11. What percentage of this potential loss to information assets is self-insured, including captives not reinsured?	APJ 2017
Less than 5%	1%
5% to 10%	3%
11% to 20%	1%
21% to 30%	3%
31% to 40%	8%
41% to 50%	9%
51% to 60%	17%
61% to 70%	17%
71% to 80%	25%
81% to 90%	9%
91% to 100%	8%
Total	100%
Extrapolated value	0.62

Q12. What is the likelihood your company will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months?	APJ 2017
Less than 0.1%	2%
0.1% to 0.5%	3%
0.6% to 1.0%	3%
1.1% to 2.0%	9%
2.1% to 3.0%	8%
3.1% to 4.0%	19%
4.1% to 5.0%	16%
5.1% to 10.0%	20%
More than 10.0%	20%
Total	100%
Extrapolated value	5.5%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months?	APJ 2017
Less than 0.1%	11%
0.1% to 0.5%	10%
0.6% to 1.0%	10%
1.1% to 2.0%	11%
2.1% to 3.0%	16%
3.1% to 4.0%	16%
4.1% to 5.0%	17%
5.1% to 10.0%	6%
More than 10.0%	3%
Total	100%
Extrapolated value	2.8%

Q14. In your opinion, how would your company disclose a material loss to information assets that is not covered by insurance in its financial statements?	APJ 2017
Disclosure as a contingent liability on the balance sheet (FASB 5)	11%
Footnote disclosure in the financial statements	42%
Discussion in the management letter	8%
None – disclosure is not necessary	35%
Other	4%
Total	100%

Part 2. Other Questions

Q15. Are you aware of the economic and legal consequences resulting from a data breach or security exploit in other countries in which your company operates, such as the European Union's General Data Protection Regulation (GDPR), which may issue a fine of up to 5 percent of an organization's worldwide revenue?	APJ 2017
Yes, fully aware	27%
Yes, somewhat aware	54%
Not aware	19%
Total	100%

Q16a. Has your company experienced a material or significantly disruptive security exploit or data breach one or more times over the past 24 months? Please refer to the definition of materiality provided above.	APJ 2017
Yes	41%
No [skip to Q17]	59%
Total	100%

Q16b. If yes, what best describes the data breaches or security exploits experienced by your company over the past 24 months? Please select all that apply.	APJ 2017
Cyber attack that caused disruption to business and IT operations (such as denial of service attacks)	46%
Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims	34%
Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties	40%
Negligence or mistakes that resulted in the loss of business confidential information	39%
System or business process failures that caused disruption to business operations (e.g. software updates)	54%
Other	5%
Total	218%

Q16c. If yes, what was the total financial impact of security exploits and data breaches experienced by your company over the past 24 months. Please include all costs including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.	APJ 2017
Zero	0%
Less than $10,000	10%
$10,001 to $100,000	12%
$100,001 to $250,000	14%
$250,001 to $500,000	27%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	10%
$5,000,001 to $10,000,000	6%
$10,000,001 to $25,000,000	5%
$25,000,001 to $50,000,000	2%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	3,314,550

Q16d. If yes, how has the above security exploit or data breach changed your company's concerns about cyber liability?	APJ 2017
More concerned	64%
Less concerned	13%
No change	23%
Total	100%

Q17. Do you believe your company's exposure to cyber risk will increase, decrease or stay the same over the next 24 months?	APJ 2017
Increase	62%
Decrease	11%
Stay the same	27%
Total	100%

Q18a. From a business risk perspective, how do cyber risks compare to other business risks. Please select one best choice.	APJ 2017
Cyber liability is the number one or two business risk for my company	18%
Cyber liability is a top 5 business risk for my company	28%
Cyber liability is a top 10 business risk for my company	40%
Cyber liability is not in the top 10 of business risks for my company	14%
Total	100%

Q18b. How did you determine the level of cyber risk to your company?	APJ 2017
Completed a formal internal assessment	16%
Completed an informal (ad hoc) internal assessment	23%
Hired a third party to conduct an assessment or audit	35%
Intuition or gut feel	15%
Did not do any type of assessment	12%
Total	100%

Q19a. Does your company have cyber insurance coverage, including within a technology Errors & Omission or similar policy not including Property, General Liability or Crime policy?	APJ 2017
Yes	18%
No [skip to Q20a]	82%
Total	100%

Q19b. If yes, what limits do you purchase	APJ 2017
Less than $1 million	5%
$1 million to $5 million	39%
$6 million to $20 million	48%
$21 million to $100 million	6%
More than $100 million	2%
Total	100%

Q19c. Is your company's cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	APJ 2017
Yes	61%
No	26%
Unsure	13%
Total	100%

Q19d. How does your company determine the level of coverage it deems adequate?	APJ 2017
Formal risk assessment by in-house staff	13%
Formal risk assessment conducted by the insurer	11%
Formal risk assessment by third party	26%
Informal or ad hoc risk assessment	12%
Policy terms and conditions reviewed by a third-party specialist	17%
Maximum available from the insurance market	21%
Other	0%
Total	100%

Q19e. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	APJ 2017
External attacks by cyber criminals	85%
Malicious or criminal insiders	81%
System or business process failures	48%
Human error, mistakes and negligence	32%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	42%
Other	30%
Total	317%

Q19f. What coverage does this insurance offer your company? Please select all that apply.	APJ 2017
Forensics and investigative costs	55%
Notification costs to data breach victims	55%
Communication costs to regulators	53%
Employee productivity losses	59%
Replacement of lost or damaged equipment	59%
Revenue losses	29%
Legal defense costs	52%
Regulatory penalties and fines	52%
Third-party liability	45%
Brand damages	24%
Other	21%
Unsure	29%
Total	532%

Q19g. In addition to cost coverage, what other services does the cyber insurer provide your company in the event of a security exploit or data breach? Please check all that apply.	APJ 2017
Access to cyber security forensic experts	73%
Access to legal and regulatory experts	74%
Access to specialized technologies and tools	52%
Advanced warnings about ongoing threats and vulnerabilities	40%
Assistance in the remediation of the incident	43%
Assistance in the notification of breach victims	51%
Identity protection services for breach victims	24%
Credit monitoring services for breach victims	40%
Assistance in reputation management activities	52%
Other	21%
Total	469%

Q20a. Does your company plan to purchase standalone cyber insurance?	APJ 2017
Yes, in the next 12 months	12%
Yes, in the next 24 months	27%
Yes, in more than 24 months	20%
No	41%
Total	100%

Q20b. If no, what are the main reasons why your company is not planning to purchase standalone cyber security insurance?	APJ 2017
Premiums are too expensive	34%
Coverage is inadequate based on our exposure	41%
Too many exclusions, restrictions and uninsurable risks	26%
Risk does not warrant insurance	9%
Property and casualty policies are sufficient	32%
Executive management does not see the value of this insurance	23%
Unable to get insurance underwritten because of current risk profile	14%
Other	6%
Total	186%

Q21. Who in your company is most responsible for cyber risk management? Please select your one top choice.	APJ 2017
CEO/board of directors	0%
Chief financial officer	5%
Business unit (LOB) leaders	21%
Chief information officer	27%
Chief information security officer	17%
Risk management	11%
Procurement	6%
General counsel	9%
Compliance/audit	2%
Other	2%
Total	100%

Part 3. Role & Organizational Characteristics

D1. What level best describes your current position?	APJ 2017
Senior executive	3%
Vice president	4%
Director	13%
Manager	14%
Supervisor	14%
Associate/staff	13%
Technician	33%
Contractor/consultant	6%
Other	0%
Total	100%

D2. What is the worldwide employee headcount of your company?	APJ 2017
Less than 500	19%
500 to 1,000	16%
1,001 to 5,000	25%
5,001 to 25,000	27%
25,001 to 75,000	9%
More than 75,000	4%
Total	100%

D3. What best describes your company's industry focus?	APJ 2017
Agriculture & food service	1%
Communications	2%
Consumer products	8%
Defense & aerospace	0%
Education & research	3%
Energy & utilities	4%
Entertainment & media	2%
Financial services	15%
Health & pharmaceuticals	7%
Hospitality	2%
Industrial	11%
Other	2%
Public sector	12%
Retail	11%
Services	13%
Technology & software	5%
Transportation	3%
Total	100%

ACKNOWLEDGEMENTS

We appreciate the past review and input of Massachusetts Institute of Technology 2016 Graduate, Adam Kalinich, major Course 18C: "Mathematics with Computer Science."

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.